Hindawi
Security and Communication Networks
Volume 2021, Article ID 8066200, 8 pages
https://doi.org/10.1155/2021/8066200

Research Article

Can Wavelet Transform Detect LDDoS Abnormal Traffic in Multipath TCP Transmission System?

Gang Lei, Lejun Ji, Ruiwen Ji, Yuanlong Cao, Wei Yang, and Hao Wang

School of Software, Jiangxi Normal University, Nanchang 330022, China

Correspondence should be addressed to Yuanlong Cao; ylcao@jxnu.edu.cn

Received 26 October 2021; Revised 28 November 2021; Accepted 29 November 2021; Published 26 December 2021

Academic Editor: Zhe-Li Liu

With the rapid development of mobile Internet technology and multihost terminal devices, multipath transmission protocol has been widely concerned. Among them, multipath TCP (MPTCP) has become a hot research protocol in recent years because of its good transmission performance and Internet compatibility. Due to the increasing power of Low-Rate Distributed Denial of Service (LDDoS) attack, the network security situation is becoming increasingly serious. The robustness of MPTCP network has become an urgent performance index to improve. Therefore, it is very necessary to detect LDDoS abnormal traffic timely and effectively in the transmission system based on MPTCP. This paper tries to use wavelet transform technology to decompose and reconstruct network traffic and find a detection method of LDDoS abnormal traffic in the MPTCP transmission system. The experimental results show that in the MPTCP transmission system, the signal processing technology based on wavelet transform can realize the identification of LDDoS abnormal traffic. It indicates a direction worth further exploration for the detection and defense of the LDDoS attack.

1. Introduction

1.1. Background. With the boom in emerging technologies such as mobile communication networks and big data, more and more communication devices are configured with multiple network interfaces (WiFi, 4G/5G, Bluetooth, and so on) [1, 2]. In order to adapt to the current rapid development of communication technology and meet the actual needs of multihost terminal users, the Internet Engineering Task Force (IETF) has published multipath transmission protocols, such as Stream Control Transmission Protocol (SCTP) [3] and multipath TCP (MPTCP) [4]. In a multipath transmission system, multipath transmission protocols allow the end user to communicate with the server end-to-end through multiple paths at the same time, realizing parallel multipath transmission. Compared with TCP and other single-path transmission protocols, this improves the throughput of the transmission system [5]. Applying multipath transmission protocols can achieve the bandwidth aggregation and load balancing of the transmission system.

However, in the face of increasingly complex and severe network security situation, the network security problem of multipath transmission protocols will be an urgent challenge [6, 7]. With the continuous expansion of computer scale and application field, the malicious attack behavior in the network presents the characteristics of fast development and diversified attack types, causing immeasurable great harm to the communication network. Among them, Denial of Service (DoS) attack [8] has evolved from Distributed Denial of Service (DDoS) attack [9, 10] to Low-Rate Distributed Denial of Service (LDDoS) attack, which poses a great threat to network security. LDDoS, a new attack type, uses a large number of dummy computers in the network to attack the target network concurrently at a low-rate, causing great harm to the target network in a short time [11]. However, due to the characteristics of low-rate and distributed, it is difficult to detect the LDDoS attack due to its strong concealment [12]. Therefore, fast and accurate detection of LDDoS abnormal traffic is one of the preconditions to ensure network security and effective operation in the multipath

transmission system. At the same time, we also need to make a rapid and reasonable response to LDDoS abnormal traffic.

A large number of studies have shown that large-scale network traffic has almost all the characteristics of signals, such as self-similarity and correlation. Self-similar data simply have the characteristics of scale invariance and slow decay of autocorrelation function. In addition, some studies have found that attack traffic (abnormal traffic) will have a significant impact on the normal network traffic. Therefore, we can regard the network data flow in the multipath transmission system as a signal and use signal analysis technology to process and analyze it, trying to find a way to detect LDDoS abnormal traffic.

1.2. Our Work. In the preliminary work [13], we built a network topology of the multipath transmission system through the NS2 (Network Simulator version 2) experimental platform. MPTCP and SCTP are applied in the multipath transmission system, respectively. Meanwhile, LDDoS attacks with the same intensity are simulated to attack MPTCP and SCTP transmission systems. We compared and analyzed throughput, delay, and jitter rate performances of MPTCP and SCTP transmission systems. Thus, we can indirectly compare the robustness of MPTCP and SCTP against the LDDoS attack. From the perspective of data scheduling and congestion control, we compared and analyzed the experimental results. Finally, we came to the following two conclusions:

(i) According to the multistream feature of SCTP and the sequential packet delivery mechanism of MPTCP, the throughput fluctuation of the MPTCP transmission system is greater than that of the SCTP transmission system. However, the average throughput of the MPTCP transmission system is higher.

(ii) The delay and jitter rate of the SCTP transmission system can always be in a state of frequent fluctuations, while the MPTCP transmission system can achieve reliable parallel multiplexing, so its stability is superior to that of the SCTP transmission system.

In conclusion, the MPTCP transmission system is more robust to LDDoS attacks than the SCTP transmission system. In addition, MPTCP has good Internet compatibility [14], so it has been widely studied and applied in recent years. Even so, LDDoS attacks can still affect the normal data transmission of the MPTCP transmission system. It is very necessary to detect LDDoS attacks quickly and accurately in network traffic of the MPTCP transmission system.

Combined with the current research status and development trend, this paper introduces the wavelet analysis method into the anomaly detection of LDDoS attacks in the MPTCP transmission system for the first time. The wavelet analysis method is a time-frequency localization analysis method with fixed window size. Its shape, time window, and frequency window can be changed [15]. Therefore, it has unique advantages of multiresolution analysis, time-frequency localization, and fine expression in nonstationary signal processing [16]. The main research work of this paper is as follows:

(i) In the simulation platform, this paper simulates the situation of LDDoS attacks on the MPTCP transmission system. According to the self-similarity of signals, both normal traffic and attack traffic in the transmission system are treated as signals.

(ii) We use discrete wavelet transform (DWT) method and Haar wavelet basis to decompose network traffic signals and extract component sequences of different frequency ranges. We analyze the data characteristics of abnormal traffic which are different from normal traffic, so as to realize the identification of LDDoS abnormal traffic in the MPTCP transmission system.

(iii) We carry out wavelet reconstruction for the approximate signals obtained by wavelet decomposition and calculate the reconstruction error, which is used to characterize the fitting degree of the original signal and the reconstructed signal.

The experimental results show that the signal processing technology based on wavelet transform (WT) can more clearly and intuitively observe the changing trend of LDDoS attacks. Thus, this can realize the identification of LDDoS abnormal traffic in the MPTCP transmission system and further improve the robustness of the MPTCP transmission system against LDDoS attacks.

The rest of this paper is organized as follows. In section II, we mainly introduce the research related to MPTCP security. In section III, we provide a detailed overview of wavelet transform methods, including the basic concepts and working principles of WT, DWT, and Haar wavelet. In section IV, we elaborate and analyze the simulation experiment and experimental results and draw the final conclusion through experimental comparison. In section V, we summarize the paper and look forward to the future work and challenges.

2. Related Work

In recent years, MPTCP has been widely studied and applied by many researchers in the field of academic research. At present, the research hotspots of MPTCP are mainly distributed in congestion control [17, 18], data scheduling [19], path management [20, 21], and energy consumption [22, 23]. However, there are relatively few research studies on MPTCP network security [14].

At present, the research on the security and robustness of MPTCP mainly focuses on defending against DoS and DDoS attacks. Chaturvedi and Chand [24] proposed a new opportunistic security protocol called Secure Connection Multipath TCP (SCMTCP). The protocol generates a unique authentication key for each new substream in the host and authenticates them using the session key to protect MPTCP from DoS attacks. Farooq et al. [25] proposed a port technology based on MPTCP to mitigate the impact of DoS

attacks in communication networks. Afzal et al. [26] proposed and implemented an MPTCP-aware connection tracker, which can effectively detect and prevent DoS attacks. Demir and Suri [27] proposed an active and robust extension of the MPTCP transport protocol to mitigate DoS and DDoS attacks by using a new stream hop.

To sum up, there are many research studies on DoS attacks and DDoS attacks defense and detection in the MPTCP transmission system but relatively few research studies on LDDoS attacks defense and detection. Only a few studies suggest the need to further improve the robustness of MPTCP transmission systems against LDDoS attacks. For example, Cao et al. [28] proposed MPTCP – (La/E^2), an energy-efficient MPTCP solution with LDDoS attack awareness, to avoid multipath transmission performance degradation caused by LDDoS attacks. Therefore, based on the current research status, we propose to combine the wavelet analysis method with LDDoS attacks detection to realize the identification and detection of LDDoS attacks in the MPTCP transmission system and further improve the robustness of MPTCP against LDDoS attacks.

3. Overview of Wavelet Transform Method

3.1. Wavelet Transform. WT is a signal processing and analysis method based on Fourier Transform (FT). Its basic idea is to represent or approximate a certain signal or function $f(t)$ by scaling and translating a set of wavelet functions (basis functions) and to refine the signal step by step [29]. It can meet the requirements of automatic time-frequency signal analysis and focus on any details of the signal [30], which is convenient for observation and analysis.

The general form of the wavelet function [31] is

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right), \quad a, b \in R, \tag{1}$$

where a represents the expansion factor, b represents the translation factor, and ψ is known as the basic wavelet or mother wavelet.

At present, WT can be divided into continuous wavelet transform (CWT) and DWT. For any function $f(t) \in L^2(R)$, the general form of CWT of $f(t)$ is

$$\mathrm{CWT}(a,b) = \langle f(t), \psi_{a,b}(t)\rangle = \frac{1}{\sqrt{a}}\int_{-\infty}^{+\infty} f(t)\overline{\psi}\left(\frac{t-b}{a}\right)\mathrm{d}t, \tag{2}$$

where the obtained coefficient $\mathrm{CWT}(a,b)$ is called CWT coefficient.

In CWT, expansion factor a, translation factor b, and time t are continuous. However, in the process of digital signal processing, it is often necessary to discretize the wavelet transform of continuous wavelet [15]. Generally, the expansion factor and the translation factor are discretized in the form of power series; let $a = a_0^j$ and $b = ka_0^j b_0$, where $a_0 > 1$, k, $j \in Z$. At the same time, generally let $a_0 = 2$ and $b_0 = 1$. The general form of DWT can be obtained by discretization of expansion factor and translation factor. For any function $f(t) \in L^2(R)$, the general form of DWT of $f(t)$ is

$$\begin{aligned} \psi_{j,k}(t) &= 2^{-(j/2)}\psi\left(2^{-j}t - k\right), \\ C_{j,k} &= \int_{-\infty}^{+\infty} f(t)\overline{\psi}_{j,k}(t)\mathrm{d}t. \end{aligned} \tag{3}$$

Among them, the obtained coefficient $C_{j,k}$ is called DWT coefficient.

3.2. Discrete Wavelet Transform. Signals are usually composed of low-frequency components and high frequency components. The low-frequency components generally contain the characteristics of the signal, while the high frequency components represent the details or differences of the signal. The working principle of DWT for input signal S is equivalent to filtering the signal with a set of mutual bandpass filters (low-pass filter and high-pass filter) [16]. The signal passing through this set of mutual bandpass filters produces two components. The approximate component signal corresponds to the low-frequency part of the signal, and the detail component signal corresponds to the high frequency part of the signal. The essence of DWT is to represent the signal with a series of approximate and detailed components [32].

In the decomposition process of DWT, the approximate component signals are continuously decomposed [31]. Each level is to decompose the approximate component signals of the upper level into the approximate component signals and detail component signals of the next level. With each increase in decomposition level, the sampling interval will be doubled, and the number of sampling points will be reduced by onefold [33]. After layers of decomposition, the original signal can be decomposed into many low-frequency components so that the changes in the signal can be observed on a large time scale. For an original signal S, its DWT decomposition process can be represented by the hierarchical structure in the following Figure 1 where CD_1, CD_2, and CD_3 and CA_1, CA_2, and CA_3 represent the detail component signals and approximate component signals of each layer, respectively.

In the practical application of DWT, the selection of wavelet function (wavelet base) and the determination of decomposition layers are the premise of wavelet analysis. There are many kinds of common wavelet functions, such as Haar, dbN, symN, and coifN. As for the determination of decomposition layers, it can continue to be decomposed theoretically. However, generally it is necessary to determine the appropriate decomposition layers according to the characteristics of signals and the needs of users.

3.3. Haar Wavelet. There are many kinds of common wavelet bases. We usually select Haar wavelet or Daubechies wavelet as the wavelet bases in the actual digital signal processing. The application of Haar wavelet to wavelet transform only requires simple addition or subtraction operation and does not involve multiplication operation, so the operation speed is fast [34].

Haar wavelet is the simplest of the Daubechies wavelet family, also known as one order Daubechies wavelet. Haar

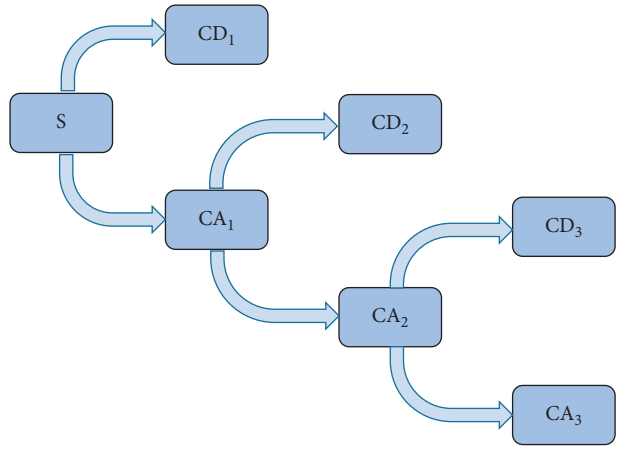

Figure 1: Hierarchical structure diagram of decomposition process of DWT.

wavelet is orthogonal wavelet with both symmetric and antisymmetric compact supports. The general form of Haar mother wavelet is

$$\psi(t) = \begin{cases} 1, & 0 \le t \le \frac{1}{2}, \\ -1, & \frac{1}{2} \le t \le 1, \\ 0, & \text{other}. \end{cases} \tag{4}$$

The general form of Haar father wavelet is

$$\phi(x) = \begin{cases} 1, & 0 \le x \le 1, \\ 0, & \text{other}. \end{cases} \tag{5}$$

Then, the Haar wavelet function can be represented by the father wavelet, as shown in the following formula:

$$\psi(t) = \phi(2t) - \phi(2t-1). \tag{6}$$

4. Simulation Experiment and Results Analysis

4.1. Simulation Experiment. In the previous work, we designed a network transmission model for MPTCP parallel transmission using NS2 platform. The network topology is shown in Figure 2 [13]. As can be seen from Figure 2, receiver can realize parallel multipath communication with sender through three paths (Path A, Path B, and Path C). In the figure, five puppet computers $(\text{Attack}_0, \ldots, \text{Attack}_4)$ can send LDDoS attack data stream to R_0, respectively, to realize network attack. The blue data flow indicates TCP normal data flow, and the red data flow indicates LDDoS attack data flow. Table 1 shows the settings of parameters such as the bandwidth of each path in the MPTCP network transmission model. All paths use the DropTail queue management algorithm, and the transfer delay is 25 ms. The bandwidth of the path between the puppet machine and the router is 1 Mb, and the bandwidth of other paths is 5 Mb.

In order to explore whether WT can identify and detect LDDoS attack traffic in the MPTCP transmission system, we adjust some original experimental settings. Based on the attack principle of LDDoS attacks, the experimental implementation of LDDoS attacks is mainly to set three important parameters of attack cycle, attack duration, and attack rate [35]. Specific parameter settings can be expressed by the following formula. Among them, the AC represents the attack cycle, AD indicates the attack duration, and AR indicates the attack rate. The LDDoS attack flow uses a CBR packet with a constant bit rate, and the packet size is 200 bytes.

$$\text{LDDoS}(\text{AC}, \text{AD}, \text{AR}) = (200\,\text{ms}, 600\,\text{ms}, 1\,\text{Mbps}). \tag{7}$$

In addition, during the overall 500 seconds running time of the experiment, we set the puppet machine to attack the MPTCP transmission system at 100 s, 200 s, 300 s, and 400 s, respectively, and the attack time lasted for 50 seconds. To ensure that the attack simulated in the experiment can achieve the best attack effect, we draw the congestion window (cwnd) change diagram of the MPTCP transmission system, as shown in Figure 3. As can be seen from the figure, the values of cwnd drop rapidly to its initial value when attacked. And during four periods of attack, the values of cwnd are always approximately equal to the initial value, that is, 1. This indicates that the LDDoS attack generated by simulation in the experiment has reached the best attack.

4.2. Results Analysis. This part attempts to perform WT decomposition on the throughput data obtained from the above simulation experiment. We try to prove that the signal analysis and processing method based on WT can identify the LDDoS attack traffic in the MPTCP transmission system. Based on this, we can further find a signal analysis and processing method that can successfully detect the LDDoS attack in the MPTCP transmission system.

If the network traffic signal is decomposed by WT, it is necessary to select the type of WT, the type of wavelet base, and the number of decomposition layers. In the process of digital signal processing, we need to adapt to the application of computer system binary, so we choose DWT to decompose. The simple and commonly used Haar wavelet is

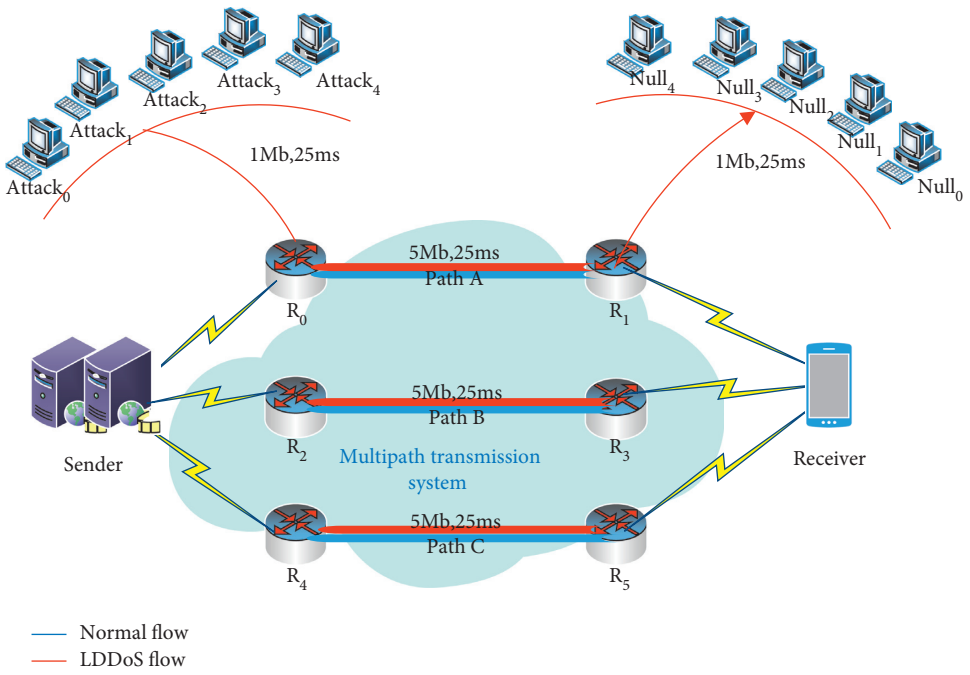

Figure 2: MPTCP transmission system network topology diagram.

Table 1: Path network parameter setting table of the MPTCP transmission system.

Path	Bandwidth (Mb)	Transfer delay (ms)	Path management algorithm
(Sender, $R_{0,2,4}$)	5	25	DropTail
($R_{1,3,5}$, receiver)	5	25	DropTail
(R_0, R_1)	5	25	DropTail
(R_2, R_3)	5	25	DropTail
(R_4, R_5)	5	25	DropTail
($\text{Attack}_{0,1,2,3,4}$, R_0)	1	25	DropTail
(R_1, $\text{Null}_{0,1,2,3,4}$)	1	25	DropTail

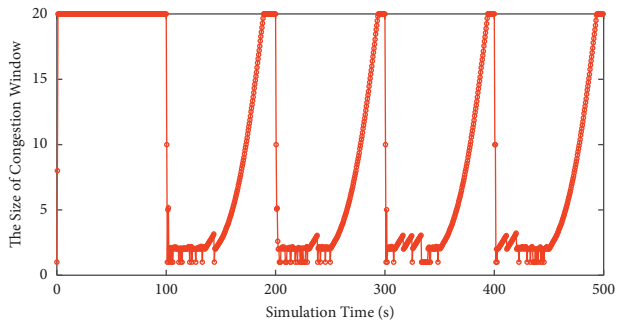

Figure 3: Congestion window change diagram of the MPTCP transmission system.

selected as wavelet base. Generally speaking, in the process of signal analysis, signal decomposition is roughly decomposed into 3 or 4 layers. So, the number of decomposition layers in our wavelet transform experiment is determined to be 3 layers.

The process of DWT can be roughly divided into signal decomposition and signal reconstruction. In the signal decomposition part, we first decompose the original signal to obtain the signal of level 1 approximate component and level 1 detail component, as shown in Figure 4. Then, we decompose the level 1 approximate component signal to obtain the level 2 approximate component signal and the level 2 detail component signal, as shown in Figure 5. Finally, in the third stage, we decompose the level 2 approximate component signal to obtain the signal of level 3 approximate component and level 3 detail component, as shown in Figure 6. The final level 3 approximate component signal is the approximate signal of the original signal obtained by the 3-layer wavelet decomposition.

Through comparative analysis of Figures 4–6, we can find that each level of decomposition is the observation of the original signal at different time scales. Due to the reduction in the number of samples, the time scale is doubled. So, some details of the signal are gradually amplified. In this way, we can observe the characteristics of the signal from a large time scale, which reflects the advantages of multiscale frequency domain analysis of DWT.

Figure 7 shows the comparison between the original signal and the approximate signal. As can be seen from Figure 7, this experiment simulates four LDDoS attacks on the MPTCP transmission system, and the duration of each

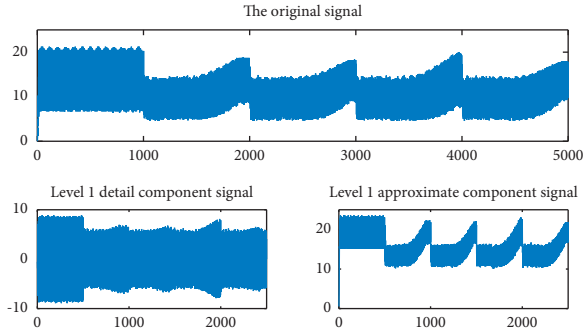

Figure 4: Comparison diagram of the original signal and the level 1 approximation component signal.

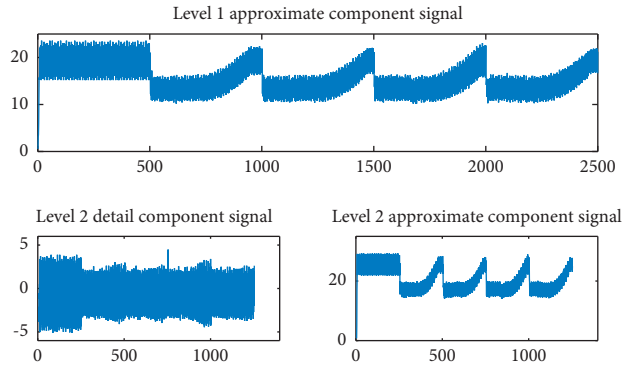

Figure 5: Comparison diagram of the level 1 and level 2 approximation component signal.

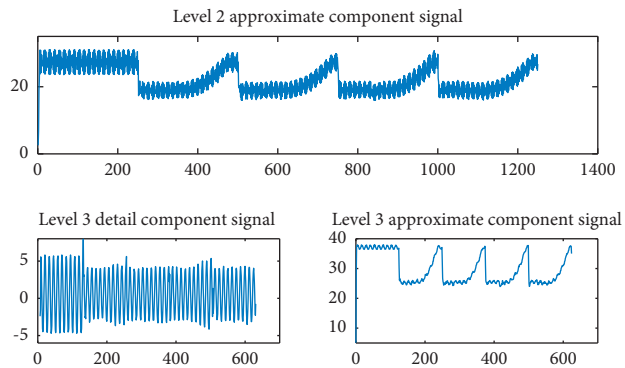

Figure 6: Comparison diagram of the level 2 and level 3 approximate component signal.

attack is 50 seconds. When the transmission system is attacked by LDDoS attacks, the throughput performance of the system will be greatly reduced. Compared with the original signal, the approximate signal decomposed by DWT can more clearly and intuitively see the attack trend and attack cycle of the LDDoS attack. In addition, we use different wavelet functions to decompose the original signal and eventually obtain the similar result. For more complex network traffic signals in real life, the wavelet analysis method can be used to decompose the complex signals into simple and clear signals. In this way, we can observe the

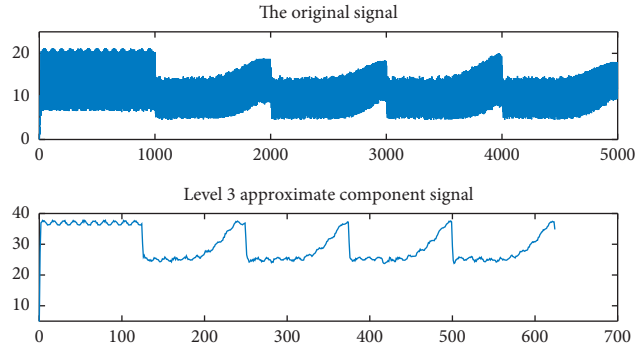

Figure 7: Comparison diagram of the original signal and the approximate signal.

slight changes of the signal, which is convenient for us to effectively extract the characteristic information from the signal. This can lay a foundation for the detection of the LDDoS abnormal traffic in the next step.

Figure 8 shows the signal process of wavelet reconstruction. In the part of signal reconstruction, we still use Haar wavelet function for wavelet reconstruction. Similar to wavelet decomposition, wavelet reconstruction works by applying a set of high-pass filter and low-pass filter. The approximate component signals and detail component signals obtained by wavelet decomposition are reconstructed gradually through the set of filters. The reconstruction sequence is reversed in accordance with the sequence shown in Figure 1; that is, the reconstruction sequence is reversed in accordance with the sequence of signal decomposition. The final reconstructed signal has the same length and shape as the original signal.

Figure 9 shows the comparison between the original signal and the reconstructed signal. As can be seen from Figure 9, compared with the original signal, the reconstructed signal is similar to the original signal in terms of variation trend, amplitude, and peak value. This shows that wavelet reconstruction can reconstruct the original signal from the recorded data without losing important information in the process of transformation and reconstruction.

In addition, we define the variable err as the reconstruction error. It represents the degree of fitting between the reconstructed signal and the original signal. Its value can be calculated by

$$\text{err} = \max\left|S - A_0\right|, \tag{8}$$

where S is the original signal and A_0 is the reconstructed signal after decomposition and reconstruction using DWT. The smaller the value is, the better the fitting degree of the reconstructed signal and the original signal is. The err obtained by calculation and solution of the experiment is 1.4211×10^{-14}, indicating that the reconstructed signal fits the original signal well. Therefore, the signal processing and analysis technology based on WT can realize the identification of LDDoS abnormal traffic in the MPTCP transmission system and then be applied to the abnormal detection of network traffic.

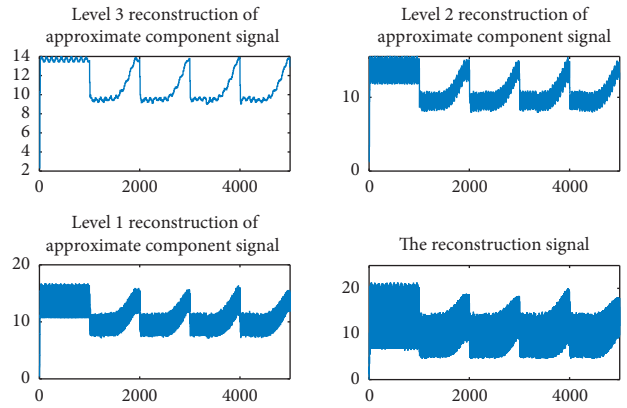

Figure 8: Wavelet reconstruction signal process diagram.

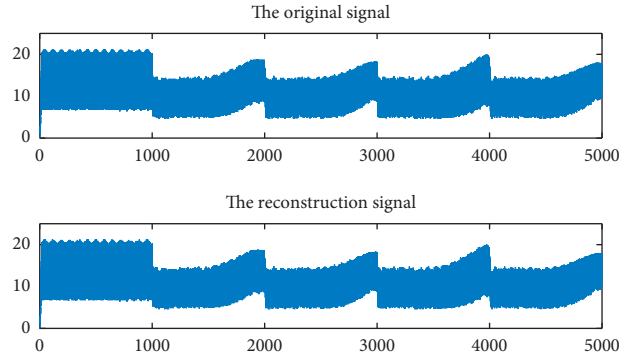

Figure 9: Comparison diagram of the original signal and the reconstructed signal.

5. Conclusion and Prospect

In this paper, we simulate the network environment of the MPTCP transmission system under LDDoS attacks and use the DWT method to decompose and reconstruct the traffic signal in the transmission system. By comparing the original signal, the approximate signal, and the reconstructed signal, we can observe the attack trend, amplitude change, and attack time of the LDDoS attack more clearly and intuitively, and the reconstructed signal has a good fitting degree with the original signal. Therefore, the analysis of wavelet decomposition and wavelet reconstruction proves that the signal processing and analysis method based on WT can realize the identification and detection of LDDoS abnormal traffic in the MPTCP transmission system.

The research results provide a new research idea in network anomaly monitoring, traffic characteristics detection, and other aspects. Thus, it can further improve the robustness of the MPTCP transmission system. In the future research work, we will use the wavelet coefficient variance method to solve self-similarity exponent (Hurst) [34] of network traffic signals on the basis of wavelet decomposition and reconstruction. Abnormal traffic in the transmission system can be judged according to the change of Hurst exponent so as to realize the real-time detection and location of LDDoS attacks in the MPTCP transmission system [35] and reduce the occurrence of abnormal traffic missing and false positives.

Data Availability

No data were used to support this article.

Conflicts of Interest

The author(s) declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant no. 61962026, by the Natural Science Foundation of Jiangxi Province under Grant no. 20192ACBL21031, by the ROIS NII Open Collaborative Research 2021 under Grant no. 21AF03, and by the Cooperative Research Project Program of the Research Institute of Electrical Communication, Tohoku University.

References

[1] S. R. Pokhrel, J. Jin, and H. L. Vu, "Mobility-aware multipath communication for unmanned aerial surveillance systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 6088–6098, 2019.

[2] K. Phejrsuksai and S. Pattaramalai, "Performance comparison of multipath TCP data transferring in bottleneck and disjoint-path wired networks connected with Wi-Fi," *in Proceedings of 2017 International Electrical Engineering Congress (iEECON)*, Pattaya, Thailand, pp. 1–4, March 2017.

[3] G. N. Vivekananda, C. P. Reddy, and A. Ilknur, "A congestion avoidance mechanism in multimedia transmission over MANET using SCTP multi-streaming," *Multimedia Tools and Applications*, vol. 79, no. 23–24, pp. 16823–16844, 2020.

[4] J.-P. Sheu, L.-W. Liu, R. Jagadeesha, and Y.-C. Chang, "An efficient multipath routing algorithm for multipath TCP in Software-Defined Networks," in *Proceedings of the 2016 European Conference on Networks and Communications (EuCNC)*, pp. 371–376, IEEE, Athens, Greece, June 2016.

[5] C. Lee, S. Song, H. Cho, G. Lim, and J.-M. Chung, "Optimal multipath TCP offloading over 5G NR and LTE networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 293–296, 2019.

[6] Y. Cao, R. Ji, L. Ji, M. Bao, L. Tao, and W. Yang, "Can multipath TCP Be robust to cyber attacks? A measuring study of MPTCP with active queue management algorithms," *Security and Communication Networks*, vol. 2021, p. 9963829, 2021.

[7] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *Journal of Internet Services and Information Security*, vol. 10, no. 2, pp. 1–15, 2020.

[8] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 741–752, 2020.

[9] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[10] O. V. Baranov, N. V. Smirnov, T. E. Smirnova, and Y. V. Zholobov, "Design of a quadrocopter with PID-controlled fail-safe algorithm," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 11, no. 2, pp. 23–33, 2020.

[11] M. Simsek and A. Senturk, "Fast and lightweight detection and filtering method for low-rate TCP targeted distributed denial of service (LDDoS) attacks," *International Journal of Communication Systems*, vol. 31, no. 18, p. e3823, 2018.

[12] G. Lei, L. Ji, R. Ji, Y. Cao, X. Shao, and X. Huang, "Extracting low-rate DDoS attack characteristics: the case of multipath TCP-based communication networks," *Wireless Communications and Mobile Computing*, vol. 2021, p. 2264187, 2021.

[13] L. Ji, G. Lei, R. Ji, Y. Cao, X. Shao, and X. Huang, "Which one is more robust to low-rate DDoS attacks? The multipath TCP or the SCTP," in *Proceedings of the 5th International Symposium on Mobile Internet Security (MobiSec'21)*, IEEE, Jeju Island, South Korea, October 2021.

[14] C. Pearce and S. Zeadally, "Ancillary impacts of multipath TCP on current and future network security," *IEEE Internet Computing*, vol. 19, no. 5, pp. 58–65, 2015.

[15] W. Qiao, W. Tian, Y. Tian, Q. Yang, Y. Wang, and J. Zhang, "The forecasting of PM2.5 using a hybrid model based on wavelet transform and an improved deep learning algorithm," *IEEE Access*, vol. 7, pp. 142814–142825, 2019.

[16] W. Deng, S. Zhang, H. Zhao, and X. Yang, "A novel fault diagnosis method based on integrating empirical wavelet transform and fuzzy entropy for motor bearing," *IEEE Access*, vol. 6, pp. 35042–35056, 2018.

[17] W. Li, H. Zhang, S. Gao, C. Xue, X. Wang, and S. Lu, "SmartCC: a reinforcement learning approach for multipath TCP congestion control in heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2621–2633, 2019.

[18] I. Mahmud, T. Lubna, Y.-J. Song, and Y.-Z. Cho, "Coupled multipath bbr (C-mpbbr): a efficient congestion control algorithm for multipath TCP," *IEEE Access*, vol. 8, pp. 165497–165511, 2020.

[19] W. Wei, K. Xue, J. Han, Y. Xing, D. S. L. Wei, and P. Hong, "BBR-based congestion control and packet scheduling for bottleneck fairness considered multipath TCP in heterogeneous wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 914–927, 2021.

[20] S. R. Pokhrel, M. Panda, and H. L. Vu, "Fair coexistence of regular and multipath TCP over wireless last-miles," *IEEE Transactions on Mobile Computing*, vol. 18, no. 3, pp. 574–587, 2019.

[21] Y. Cao, D. Yu, L. Zeng et al., "Towards efficient parallel multipathing: a receiver-centric cross-layer solution to aid multipath TCP," in *Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 790–797, IEEE, Tianjin, China, December 2019.

[22] J. Wu, B. Cheng, M. Wang, and J. Chen, "Quality-aware energy optimization in wireless video communication with multipath TCP," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2701–2718, 2017.

[23] Y. Khamayseh, W. Mardini, M. Aldwairi, and H. Mouftah, "On the optimality of route selection in grid wireless sensor networks: theory and applications," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 11, no. 2, pp. 87–105, 2020.

[24] R. K. Chaturvedi and S. Chand, "Multipath TCP security over different attacks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 9, p. e4081, 2020.

[25] S. M. Farooq, S. Nabirasool, S. Kiran, S. M. Suhail Hussain, and T. S. Ustun, "MPTCP based mitigation of denial of service (DoS) attack in PMU communication networks," in *Proceedings of the 2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, pp. 1–5, IEEE, Chennai, India, December 2018.

[26] Z. Afzal, S. Lindskog, A. Brunstrom, and A. Liden, "Towards multipath TCP aware security technologies," in *Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–8, IFIP, Larnaca, Cyprus, November 2016.

[27] K. Demir and N. Suri, "Towards DDoS attack resilient wide area monitoring systems," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pp. 1–7, Reggio Calabria, Italy, August, 2017.

[28] Y. Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS-aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE Access*, vol. 5, pp. 21862–21872, 2017.

[29] H. Pan, Y. Yang, X. Li, J. Zheng, and J. Cheng, "Symplectic geometry mode decomposition and its application to rotating machinery compound fault diagnosis," *Mechanical Systems and Signal Processing*, vol. 114, pp. 189–211, 2019.

[30] S. A. Raza, A. Sharif, W. K. Wong, and M. Z. A. Karim, "Tourism development and environmental degradation in the United States: evidence from wavelet-based analysis," *Current Issues in Tourism*, vol. 20, no. 16, pp. 1768–1790, 2017.

[31] S. Aasim, S. N. Singh, and A. Mohapatra, "Repeated wavelet transform based ARIMA model for very short-term wind speed forecasting," *Renewable Energy*, vol. 136, pp. 758–768, 2019.

[32] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4863–4882, 2018.

[33] E. Alickovic, J. Kevric, and A. Subasi, "Performance evaluation of empirical mode decomposition, discrete wavelet transform, and wavelet packed decomposition for automated epileptic seizure detection and prediction," *Biomedical Signal Processing and Control*, vol. 39, pp. 94–102, 2018.

[34] M. Garcin, "Hurst exponents and delampertized fractional brownian motions," *International Journal of Theoretical and Applied Finance*, vol. 22, no. 5, p. 1950024, 2019.

[35] M. Alizadeh, K. Andersson, and O. Schelen, "A survey of secure Internet of things in relation to blockchain," *Journal of Internet Services and Information Security*, vol. 10, no. 3, pp. 47–75, 2020.